Enhanced Physical Layer Security Through Transmit Antenna Selection

Hirley Alves, Richard Demo Souza, Merouane Debbah

Enhanced Physical Layer Security Through Transmit Antenna Selection

Hirley Alves and Richard Demo Souza
Federal University of Technology - Paraná (UTFPR)
Curitiba, Brazil.
hirley@ieee.org, richard@utfpr.edu.br

Mérouane Debbah
Alcatel-Lucent Chair on Flexible Radio, SUPELEC
Gif-sur-Yvette, France.
merouane.debbah@supelec.fr

***Abstract*—We analyze the physical layer security of a communication scheme with a multiple antenna legitimate transmitter, employing transmit antenna selection (TAS), and a single antenna legitimate receiver in the presence of a single antenna eavesdropper. We developed closed-form expressions for the analysis of the secrecy outage probability supposing independent and quasi-static Rayleigh fading channels. Our results show that the secrecy outage probability is considerably increased when multiple antennas are available at the legitimate transmitter. Moreover, due to the use of the TAS technique, the eavesdropper is not able to exploit the additional spatial diversity offered by the legitimate transmitter.**

I. Introduction

The broadcast nature of the wireless medium rises several security issues, once anyone within the communication range can overhear the transmission and possibly extract some information. Cryptographic techniques relying on secret keys have been widely used to assure confidentiality [1]. However, those techniques rely on the limited computational power of the eavesdropper, which however is rising at a very fast pace. Moreover, complex protocols are needed to assure the distribution and maintenance of the secret keys.

Physical layer security was pioneered by Shannon [2]. Later, in [3], Wyner introduced the wiretap channel and proved that there are channel codes that guarantee both low error probabilities and a certain degree of confidentiality. In the wiretap channel, two legitimate users, commonly known as Alice and Bob, communicate in the presence of an eavesdropper, known as Eve. Alice and Bob communicate through the main channel while Eve observes through the eavesdropper channel a degraded version of the message seen by Bob. In [3], [4] it was demonstrated that the secrecy capacity on a Gaussian wiretap channel can be defined as the difference between the capacity of the main channel and the eavesdropper channel, considering that the capacity of the former is greater than the later. In [5], [6] the authors have studied the secrecy capacity and secrecy outage probability when the wiretap channel is a quasi-static Rayleigh fading channel.

Recently, in [7] secrecy capacity expressions were derived to the Gaussian Multiple Input Multiple Output (MIMO) wiretap channel, also known as MIMOME channel, where the Alice, Bob and Eve are assumed to have multiple antennas. A different scenario was analyzed in [8] in which only the eavesdropper has multiple antennas and the channels are subject to quasi-static Rayleigh fading. The authors in [8] have shown that, from a secrecy point of view and when Selection Combining (SC) is taken into account, a single multiple antenna eavesdropper causes the same effect of multiple single antenna eavesdroppers. Moreover, it was shown that the secrecy outage probability rises as the number of the eavesdropper antennas increases. The authors also compared SC to Maximal Ratio Combining (MRC) at the eavesdropper. Their results show that MRC is more efficient than SC, which means that the eavesdropper may be more dangerous by employing MRC (would be more successful in extracting information from the signal sent from Alice to Bob). By its turn, in [9] both Bob and Eve are assumed to have multiple antennas while Alice is a single antenna device. The authors developed closed-form expressions for the secrecy outage probability, considering that the receivers employ MRC. The results show that the use of multiple receive antennas can enhance security, and that the secrecy outage probability is a function of the ratio between the number of receive antennas at Bob and Eve.

Instead, in this work we assume that only Alice has multiple antennas and that Bob and Eve are single antenna devices. For instance, in practice Alice can be seen as a base station in a cellular network, while Bob and Eve may be regular mobile users. Therefore, due to size and cost limitations it is reasonable to assume that they are single antenna devices. We assume that Alice employs Transmit Antenna Selection (TAS), and that Bob informs Alice of the best antenna index through an open (non-secure) and low rate return channel. Although Eve is able to access the open return channel, it will not be able to exploit this information since Eve has access uniquely to the the antenna index, not to anything related to the information. Moreover, such an antenna index is optimum for the main channel only. Therefore, Eve is not able to exploit any additional diversity from the multiple transmit antennas at Alice. The main contributions of this paper are the closed-form expressions derived to the secrecy outage probability and to show that physical layer security can be considerably enhanced through of the use of TAS at Alice.

The rest of this paper is organized as follows. Section II introduces the system model. In Section III the closed-form expressions for the analysis of the secrecy outage probability are derived. Section IV presents secrecy outage probability numerical results. Finally, Section V concludes the paper.

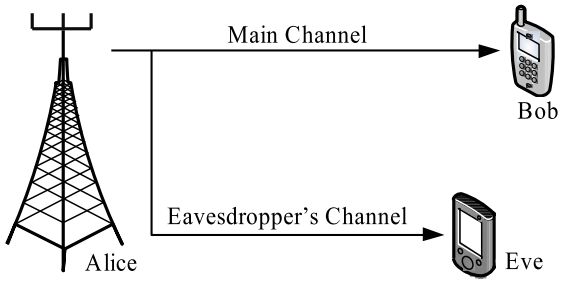

Fig. 1. System Model. Alice is the Base Station, while the receivers, Bob and Eve, are regular users of the cellular network.

II. System Model

We consider that Alice has L_A antennas and that Bob and Eve are single antenna devices. For instance Alice could be the base station of a cellular network, while Bob and Eve are regular users, as illustrated in Fig. 1. All channels are assumed to be quasi-static Rayleigh fading channels, and all noise vectors are zero-mean circularly symmetric complex Gaussian. The receivers have full channel state information (CSI) of their own channels [5]. Moreover, we consider the presence of an open return channel. Through this channel Bob sends the index of Alice's antenna with the best signal to noise ratio (SNR) at Bob. Then, Alice uses this index in a TAS scheme, allowing Bob to achieve L_A diversity order. From Eve's point of view, the optimum TAS scheme for Bob seems to be a random TAS scheme, as the main channel and the eavesdropper channel are uncorrelated and Eve have no CSI of the main channel. Consequently, Eve is not capable of exploiting any additional spatial diversity, achieving a unitary diversity order.

After TAS Alice sends the message $\mathbf{x}$ to Bob. The signal vector $\mathbf{y}$ received by Bob can be written as:

$$\mathbf{y} = h_M \, \mathbf{x} + \mathbf{n}_M \tag{1}$$

where h_M is a scalar representing the Rayleigh fading coefficient of the channel between the selected antenna from Alice and the receive antenna at Bob, while $\mathbf{n}_M$ is the noise vector. By its turn, Eve is capable of eavesdropping the signal sent by Alice. Thus, the signal vector received by Eve is given by:

$$\mathbf{z} = h_W \, \mathbf{x} + \mathbf{n}_W \tag{2}$$

where h_W is the Rayleigh fading coefficient and $\mathbf{n}_W$ is the noise vector.

Now, we can write the instantaneous SNR at Bob's receiver as:

$$\gamma_M = \frac{P \kappa_M \, |h_M|^2}{N_M}, \tag{3}$$

where P is the average transmit power, κ_M is the path loss coefficient of the main channel, and N_M is the noise power of the main channel. The average SNR is $\overline{\gamma}_M = \frac{P \kappa_M E[|h_M|^2]}{N_M}$ where $E[.]$ is the mathematical expectation. Similarly, for Eve we have $\gamma_W = \frac{P \kappa_W |h_W|^2}{N_W}$, and $\overline{\gamma}_W = \frac{P \kappa_W E[|h_W|^2]}{N_W}$, where κ_W is the path loss coefficient of the eavesdropper's channel and N_W is the noise power of the eavesdropper's channel.

The probability density function (pdf) of γ_M can be written as [10]:

$$p(\gamma_M) = \frac{L_A}{\overline{\gamma}_M} \cdot \exp\left(-\frac{\gamma_M}{\overline{\gamma}_M}\right) \cdot \left[1 - \exp\left(-\frac{\gamma_M}{\overline{\gamma}_M}\right)\right]^{L_A - 1}, \quad \gamma_M > 0 \tag{4}$$

and the pdf of γ_W is

$$p(\gamma_W) = \frac{1}{\overline{\gamma}_W} \cdot \exp\left(-\frac{\gamma_W}{\overline{\gamma}_W}\right), \quad \gamma_W > 0. \tag{5}$$

As aforementioned, the instantaneous secrecy capacity can be defined as:

$$C_s = C_M - C_W \tag{6}$$

where

$$C_M = \log\left(1 + \gamma_M\right), \tag{7}$$

is the instantaneous capacity of the main channel[1]. Likewise:

$$C_W = \log\left(1 + \gamma_W\right). \tag{8}$$

Thus, based on the non-negativity of the channel capacity, we can rewrite the secrecy capacity as

$$C_s = \begin{cases} \log\left(1 + \gamma_M\right) - \log\left(1 + \gamma_W\right) & \gamma_M > \gamma_W \\ 0 & \gamma_M \leq \gamma_W \end{cases} \tag{9}$$

Considering the independence between the main channel and the eavesdropper's channel, we can derive the probability of the existence of a non-zero secrecy capacity as:

$$\begin{aligned} \mathcal{P}(C_s > 0) &= \mathcal{P}(\gamma_M > \gamma_W) \\ &= \int_0^{\infty} \int_0^{\gamma_M} p(\gamma_M, \gamma_W) d\gamma_W d\gamma_M \\ &= \int_0^{\infty} \int_0^{\gamma_M} p(\gamma_M) p(\gamma_W) d\gamma_W d\gamma_M \\ &= 1 - \frac{\Gamma\left(1 + L_A\right) \Gamma\left(\frac{\overline{\gamma}_M + \overline{\gamma}_W}{\overline{\gamma}_W}\right)}{\Gamma\left(1 + L_A + \frac{\overline{\gamma}_M}{\overline{\gamma}_W}\right)}, \end{aligned} \tag{10}$$

where $\mathcal{P}(\theta)$ is the probability of the event θ, and $p(\gamma_M, \gamma_W) = p(\gamma_M) p(\gamma_W)$ is the joint pdf of γ_M and γ_W. Moreover, $\Gamma(.)$ denotes the complete Gamma function defined as $\Gamma(s) = \int_0^{\infty} t^{s-1} e^{-t} dt$ [11, Chap. 6].

[1]In this paper log is the logarithm to base two.

$$\begin{aligned}\mathcal{P}(C_s<\mathcal{R}_s \mid \gamma_M>\gamma_W) &= \mathcal{P}([\log(1+\gamma_M)-\log(1+\gamma_W)]<\mathcal{R}_s \mid \gamma_M>\gamma_W) \\ &= \mathcal{P}(\gamma_M<\left(2^{\mathcal{R}_s}(1+\gamma_W)-1\right) \mid \gamma_M>\gamma_W) = \int_0^{\infty}\int_{\gamma_W}^{\left(2^{\mathcal{R}_s}(1+\gamma_W)-1\right)} \frac{p(\gamma_M)\,p(\gamma_W)}{\mathcal{P}(\gamma_M>\gamma_W)} d\gamma_M d\gamma_W \\ &= \frac{-\overline{\gamma}_M\Gamma(1+L_A)\,\Gamma\left(\frac{\overline{\gamma}_M}{\overline{\gamma}_W}\right)+\overline{\gamma}_W\Gamma\left(1+L_A+\frac{\overline{\gamma}_M}{\overline{\gamma}_W}\right)\,{}_2F_1\left(-L_A,\frac{2^{-\mathcal{R}_s}\overline{\gamma}_M}{\overline{\gamma}_W},1+\frac{2^{-\mathcal{R}_s}\overline{\gamma}_M}{\overline{\gamma}_W},e^{\frac{1-2^{\mathcal{R}_s}}{\overline{\gamma}_M}}\right)}{\overline{\gamma}_W\Gamma\left(1+L_A+\frac{\overline{\gamma}_M}{\overline{\gamma}_W}\right)-\overline{\gamma}_M\Gamma(1+L_A)\Gamma\left(\frac{\overline{\gamma}_M}{\overline{\gamma}_W}\right)}\end{aligned} \tag{14}$$

$$\begin{aligned}\mathcal{O}(\mathcal{R}_s) &= \frac{\overline{\gamma}_W\Gamma\left(1+L_A+\frac{\overline{\gamma}_M}{\overline{\gamma}_W}\right)\,{}_2F_1\left(-L_A,\frac{2^{-\mathcal{R}_s}\overline{\gamma}_M}{\overline{\gamma}_W},1+\frac{2^{-\mathcal{R}_s}\overline{\gamma}_M}{\overline{\gamma}_W},e^{\frac{1-2^{\mathcal{R}_s}}{\overline{\gamma}_M}}\right)}{\overline{\gamma}_W\Gamma\left(1+L_A+\frac{\overline{\gamma}_M}{\overline{\gamma}_W}\right)-\overline{\gamma}_M\Gamma(1+L_A)\Gamma\left(\frac{\overline{\gamma}_M}{\overline{\gamma}_W}\right)}+ \\ &\quad \frac{\Gamma(1+L_A)\left\{\overline{\gamma}_W\Gamma\left(\frac{\overline{\gamma}_M+\overline{\gamma}_W}{\overline{\gamma}_W}\right)-\overline{\gamma}_M\Gamma\left(\frac{\overline{\gamma}_M}{\overline{\gamma}_W}\right)\left[1+\,{}_2F_1\left(-L_A,\frac{2^{-\mathcal{R}_s}\overline{\gamma}_M}{\overline{\gamma}_W},1+\frac{2^{-\mathcal{R}_s}\overline{\gamma}_M}{\overline{\gamma}_W},e^{\frac{1-2^{\mathcal{R}_s}}{\overline{\gamma}_M}}\right)\right]\right\}}{\overline{\gamma}_W\Gamma\left(1+L_A+\frac{\overline{\gamma}_M}{\overline{\gamma}_W}\right)-\overline{\gamma}_M\Gamma(1+L_A)\Gamma\left(\frac{\overline{\gamma}_M}{\overline{\gamma}_W}\right)}.\end{aligned} \tag{15}$$

III. Secrecy Outage Probability

A more adequate metric to measure the performance of a quasi-static Rayleigh channel is the outage probability, which can be defined as [5], [6]:

$$\mathcal{O}(\mathcal{R}_s)=\mathcal{P}(C_s<\mathcal{R}_s), \tag{11}$$

where $\mathcal{R}_s>0$ is the secrecy rate [5], [9]. We can rewrite the secrecy outage probability as:

$$\begin{aligned}\mathcal{O}(\mathcal{R}_s) &= \mathcal{P}(C_s<\mathcal{R}_s \mid \gamma_M>\gamma_W)\mathcal{P}(\gamma_M>\gamma_W)+ \\ &\quad \mathcal{P}(C_s<\mathcal{R}_s \mid \gamma_M\le\gamma_W)\mathcal{P}(\gamma_M\le\gamma_W).\end{aligned} \tag{12}$$

Note that $C_s=0$ when $\gamma_M\le\gamma_W$ and $\mathcal{R}_s>0$, therefore $\mathcal{P}(C_s<\mathcal{R}_s \mid \gamma_M\le\gamma_W)=1$. In (10) we defined $\mathcal{P}(\gamma_M>\gamma_W)$, consequently

$$\begin{aligned}\mathcal{P}(\gamma_M\le\gamma_W) &= 1-\mathcal{P}(\gamma_M>\gamma_W) \\ &= \frac{\Gamma(1+L_A)\,\Gamma\left(\frac{\overline{\gamma}_M+\overline{\gamma}_W}{\overline{\gamma}_W}\right)}{\Gamma\left(1+L_A+\frac{\overline{\gamma}_M}{\overline{\gamma}_W}\right)}.\end{aligned} \tag{13}$$

Now, knowing that $p(\gamma_M,\gamma_W \mid \gamma_M>\gamma_W)=\frac{p(\gamma_M)p(\gamma_W)}{\mathcal{P}(\gamma_M>\gamma_W)}$, we can determine $\mathcal{P}(C_s<\mathcal{R}_s \mid \gamma_M>\gamma_W)$ as show in (14). Note that in (14) ${}_2F_1(a,b;c;z)$ is the Gauss hypergeometric function, which is defined as ${}_2F_1(a,b;c;z)=\sum_{k=0}^{\infty}\frac{(a)_k(b)_k}{(c)_k}\frac{z^k}{k!}$, in which $(.)_i$ is the Pochhammer symbol defined as $(x)_n=\frac{\Gamma(x+n)}{\Gamma(x)}$ [11, Chap. 15]. In addition, all functions used in this paper can be easily found in modern mathematical frameworks and in [11].

Finally, taking (10), (13) and (14), and then putting into (12) we have a closed-form expression for the secrecy outage probability for our proposed scheme, which is given by (15). Notice that when $L_A=1$, (15) reduces to:

$$\mathcal{O}(\mathcal{R}_s)=1-\frac{\overline{\gamma}_M}{\overline{\gamma}_M+2^{\mathcal{R}_s}\overline{\gamma}_W}\exp\left(-\frac{2^{\mathcal{R}_s}-1}{\overline{\gamma}_M}\right), \tag{16}$$

which is the same result as that in [5], where the authors considered that Alice, Bob and Eve are single antenna devices communicating over independent and quasi-static Rayleigh fading channels.

We end this section by noting that beamforming, which allows for simultaneous transmissions through all antennas, is known to outperform the other transmit diversity techniques as TAS. Nevertheless, beamforming requires complete CSI feedback from Bob to Alice, which is often not practical as it would require a very high capacity return channel [12]. Moreover, with beamforming Eve would be still able to take advantage of the spatial diversity offered by Alice's transmit antenna, unless Alice has full CSI of the eavesdropper channel, which is an even less practical assumption. Our proposed scheme, besides requiring a very low rate return channel as only a few bits have to be fed back, also guarantees that Eve will not be able to exploit the additional spatial diversity offered by Alice's antennas.

IV. Numerical Results

In this section we evaluate the performance of the proposed scheme by means of some numerical results. Fig. 2 compares the secrecy outage probability for different values of L_A, $\overline{\gamma}_W=10$dB and $\mathcal{R}_s=0.1$bits/s/Hz. From the figure we can notice that the secrecy outage probability decreases as the diversity order increases. For example, for $\mathcal{O}(\mathcal{R}_s)=10^{-2}$ a gain around 6dB in SNR is achieved by having $L_A=2$ instead of $L_A=1$. From the figure we can conclude that the system is able to support tighter security constraints when multiple antennas are available at the transmitter. Moreover, it is important to notice that Monte Carlo simulation and analytical results agree very well, confirming the correctness of the theoretical analysis.

Fig. 3 shows the secrecy outage probability for different $\overline{\gamma}_W$, assuming $L_A=4$ and target secrecy rates: $\mathcal{R}_s=0.1$bits/s/Hz and $\mathcal{R}_s=1$bits/s/Hz. The outage probability rises

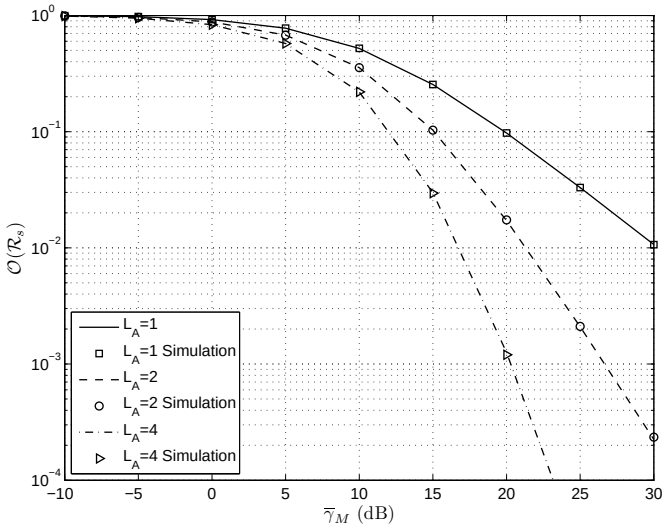

Fig. 2. Secrecy outage probability as a function of $\overline{\gamma}_M$ when $\mathcal{R}_s = 0.1$bits/s/Hz.

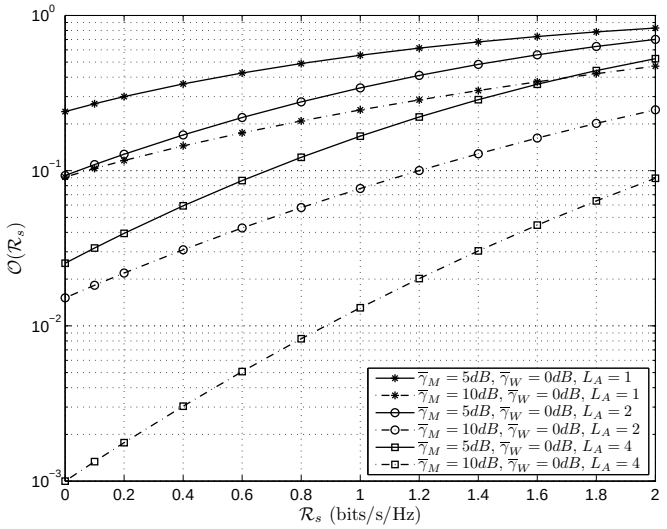

Fig. 4. Secrecy outage probability as a function of $\mathcal{R}_s$, for different $\overline{\gamma}_W$, $\overline{\gamma}_M$ and L_A.

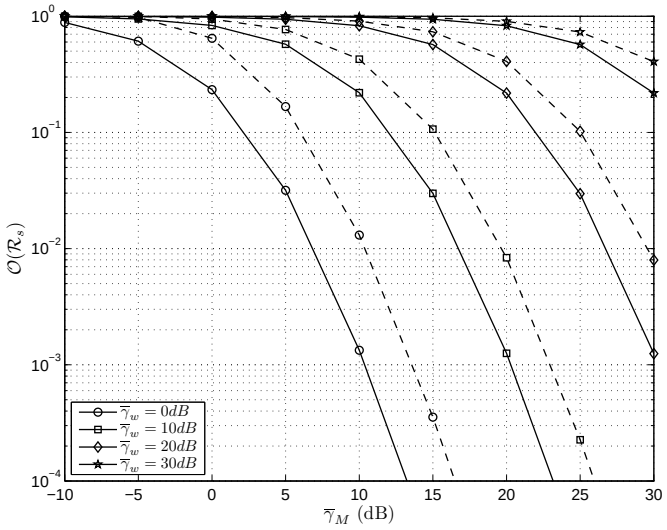

Fig. 3. Secrecy outage probability as a function of $\overline{\gamma}_M$, for different $\overline{\gamma}_W$. The solid lines and the dash lines represent, respectively, $\mathcal{R}_s = 0.1$bps/s/Hz and $\mathcal{R}_s = 1$bps/s/Hz.

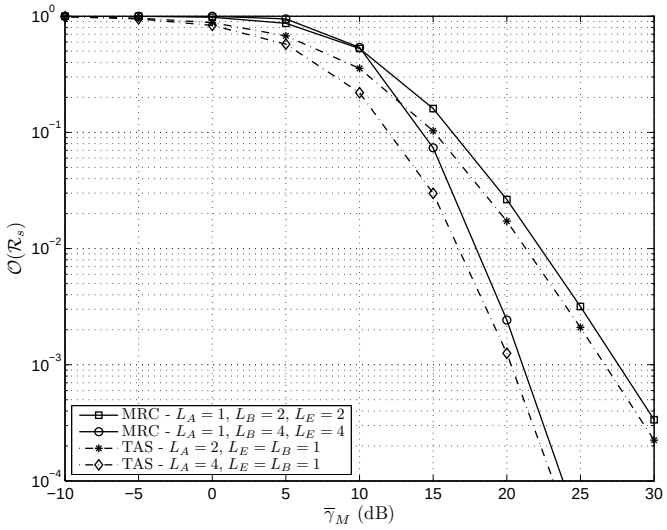

Fig. 5. Secrecy outage probability, as a function of $\overline{\gamma}_M$. We compare the performance between the proposed scheme (TAS) and that in [9] (MRC) when $\overline{\gamma}_W = 10$dB and $\mathcal{R}_s = 0.1$bits/s/Hz, and where L_B and L_E are the number of antennas at Bob and Eve.

as the average SNR of the eavesdropper channel increases. However, in the Rayleigh fading scenario it is possible to achieve a certain level of secrecy outage probability even if $\overline{\gamma}_W > \overline{\gamma}_M$, which is not possible with Gaussian channels. Consequently, a certain degree of confidentiality is achievable even if the main channel is worse than the eavesdropper channel.

Similar conclusions can be obtained when the diversity order L_A may vary as show in Fig. 4, in which the secrecy outage probability is a function of the secrecy rate $\mathcal{R}_s$. We assume that the average SNR of the eavesdropper channel is fixed to $\overline{\gamma}_W = 0$dB and the average SNR of the main channel can assume values $\overline{\gamma}_M = 5$dB and $\overline{\gamma}_M = 10$dB. From Fig. 4 we can see that to a given secrecy outage probability it is possible to achieve gains in the order of 3.5 to 4.5 times in the secrecy rate by increasing L_A or by having a stronger main channel.

In Fig. 5 we compare the proposed scheme to the one described in [9], in which the authors consider that Alice is a single antenna device, and that both Bob and Eve have multiple antennas and employ the MRC technique. From the figure, which assumes $\overline{\gamma}_W = 10$dB and $\mathcal{R}_s = 0.1$bits/s/Hz, we can see that the proposed scheme outperforms the method in [9] for all SNR. Note that the advantage is even larger at low SNR. Other values of secrecy rates were considered and

similar conclusions were obtained. Notice that in the scheme introduced in [9] both Bob and Eve are able to exploit spatial diversity. However, in our proposed scheme only Bob is able to exploit the additional spatial diversity offered by Alice[2]. Furthermore, we remark that to all results presented in this Section no more than two bits are necessary to be transmitted from Bob to Alice through the return channel. The number of bits which have to be transmitted through the return channel is $n = \lceil \log(L_A) \rceil$.

V. Conclusion

We analyzed the secrecy of a scenario in which Alice has multiple antennas while Bob and Eve are single antenna devices. A limited feedback channel is assumed between Bob and Alice, while Alice employs TAS. We developed closed-form expressions for the secrecy outage probability. Our results show that high levels of security can be achieved when the number of antennas at Alice increases. Furthermore, due to the use of TAS at Alice, Eve is not able to exploit any additional diversity offered by Alice, what is considerably beneficial in terms of secrecy.

Acknowledgments

This work was partially supported by CNPq and CAPES (Brazil).

References

[1] C. Kaufman, R. Perlman, and M. Speciner, *Network Security: Private Communication in a Public World*, 2nd ed. Prentice Hall, 2002.

[2] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, pp. 656–715, 1949.

[3] A. D. Wyner, "The wire-tap channel," *Bell Sys. Tech. J.*, vol. 54, pp. 1355 –1387, 1975.

[4] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *Information Theory, IEEE Transactions on*, vol. 24, no. 4, pp. 451 – 456, jul 1978.

[5] J. Barros and M. Rodrigues, "Secrecy capacity of wireless channels," in *2006 IEEE International Symposium on Information Theory*, 2006, pp. 356 –360.

[6] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *Information Theory, IEEE Transactions on*, vol. 54, no. 6, pp. 2515 –2534, june 2008.

[7] A. Khisti and G. Wornell, "Secure transmission with multiple antennas - part ii: The mimome wiretap channel," *Information Theory, IEEE Transactions on*, vol. 56, no. 11, pp. 5515 –5532, nov. 2010.

[8] V. Prabhu and M. Rodrigues, "On wireless channels with m-antenna eavesdroppers: Characterization of the outage probability and outage secrecy capacity," *Information Forensics and Security, IEEE Transactions on*, no. 99, 2011.

[9] F. He, H. Man, and W. Wang, "Maximal ratio diversity combining enhanced security," *IEEE Communications Letters*, vol. 15, no. 5, pp. 509 –511, 2011.

[10] A. Goldsmith, *Wireless Communications*. Cambridge University Press, 2005.

[11] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, 10th ed. Dover Publications, 1972.

[12] T. Yoo, N. Jindal, and A. Goldsmith, "Multi-antenna downlink channels with limited feedback and user selection," *Selected Areas in Communications, IEEE Journal on*, vol. 25, no. 7, pp. 1478 –1491, 2007.

[2]Note that our proposed scheme can be extended to the case where Bob and Eve have multiple receive antennas. However, even in this case Eve will not be able to exploit any additional spatial diversity from Alice's antennas.